Information-Age "De-Terror-ence"

by Mr. Timothy L. Thomas, Foreign Military Studies Office

This article appeared in

Military Review

September-October 2001

The 11 September 2001 attack on America radically changed the way nations and inter-national organizations think about terrorism. For example, President George W. Bush stated that the United States would begin a long war against terrorism, and Secretary of Defense Donald H. Rumsfeld received extra budget concessions for the counterterrorism fight. For the first time in history NATO implemented Article 5 of the 1949 Washington Treaty, which recognizes that an attack against one NATO member should be considered an attack against all members. This lifted the political constraints normally associated with using the military to fight terrorism. As the investigation unfolded, the power of information-age tools, such as the Internet, as a terrorist planning and execution asset was exposed.

The information revolution's promise of globalization and its implicit lower communication costs and integrated economies has other, more sinister, uses when placed in terrorists' hands. This article defines terrorism in the information age and examines how information enables terrorists to further their goals. Recommendations are also offered as a "de-terror-ence" policy to fight this new threat.[1]

Information Terrorism

Traditionally, terrorism focuses on using violence-threats or outright acts-to cause fear or alarm, usually for some political goal. Terrorists exploit the formal structure of the civilized world to accomplish these goals. Among other things this exploitation includes a nation-states' legal and intelligence constraints to act; its objectivity in news telecasts; and its infrastructure and operating principles. Nearly everything in the nation-state is open for its citizens to examine and use, and hence the terrorist as well. The terrorist can live in almost total anonymity until an act of

violence or crime is perpetrated. He usually trains on the very systems he will use in an attack. This enables the weak to confront and combat the strong.

A terrorist lives in the opposite world, one of near total secrecy. Usually only sketchy information is available about a terrorist's operating principles and infrastructure, if they are known at all, and the terrorist has no constraints on collecting intelligence or conducting illegal activities. Terrorists are criminals who can use indiscriminate force against populations. They realize that police or military responses may be limited because of civil liberty and security concerns. Terrorists have access to everything the average citizen does and thus are leeches who live off others to support their anger. Their methods may be deemed asymmetric because their system of operation and that of the civilized world are not comparable. Destroying the World Trade Center with a flying fuel cell, terrorizing America with anthrax-laced mail, planning to exploit the trucking industry and crop dusters to transport or spread biological or chemical agents, and killing the leader of the Northern Alliance in Afghanistan with an explosive device hidden in a camera during an interview are good examples of asymmetric tools available to terrorists.

The Federal Bureau of Investigation (FBI) defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segments thereof, in furtherance of political or social objectives."[2] In the information age, terrorism has expanded its scope and has found a ready ally in instruments such as the Internet to facilitate these efforts. Some have even coined the process of exploiting the Internet for terrorist purposes as "information terrorism," defining it as the nexus between criminal information system fraud or abuse and the physical violence of terrorism; and intentionally abusing a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action.[3] Computer attacks are the most often cited example of "the use of force or violence" in the information age because everyone is familiar with these attacks. FBI special agent Mark Pollitt defines cyberter-rorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents."[4] Cyber-terrorism uses soft violence, which is as much psychological as it is actual, to achieve its goals. Other methods of altering data can also be considered as information terrorism, such as interfering with onboard global positioning systems and causing two airliners to collide

The Internet and "Netwar"

Perhaps a more appropriate rendering for terrorism today is simply "terrorism in the information age" instead of information terrorism. For example, with regard to the Internet, a terrorist attempts to succeed by using the Internet's open promise of an integrated and cooperative world to discredit governments, degrade user confidence, and corrupt or disrupt key systems by inserting data errors or by causing intermittent shutdowns. In many cases, this produces fear or alarm and thus is a modern-day supplement to traditional terrorism. There are nine likely ways in which a terrorist group can use the Internet:

Sensitive target data. The Internet can be used to gather detailed information on targets. If a terrorist can capture sensitive data on a target as important as a pipeline or electric power grid, he

can then manipulate or blackmail businesses or governments. Concern over easy access to imagery for target planning was demonstrated immediately after 11 September as several websites removed photos and data that suddenly appeared too sensitive. On 18 October, the Pentagon purchased all rights to pictures of Afghanistan taken by Space Imaging Incorporated's IKONOS satellite, which can discern space objects as small as 1 square meter on the ground.[5]

Financial support. The Internet can be used to gather money to support a cause and to manipulate stock options that benefit terrorists through a ter-rorist attack. One of the websites dedicated to the Chechen Republic's cause in its breakaway fight against Russia, directs readers to a bank and provides the account number in which to send money to support the Chechen effort. An investigation is underway to see if there were stock deals made by the al-Qaeda network in the days preceding 11 September.

Disparate group connections. The Internet can be used to connect disparate groups. A religious sect from any country or region, or people backing a particular cause can now stay in touch. These websites provide instructions on when and where to meet or on types of protests or issues to study. That is, the Internet has a synergistic effect on such groups' activities.

Extortion. The Internet can be used to attack individuals, groups, or companies, such as financial institutions, or to directly lobby decisionmakers. Extortionists use the Internet to extort money from financial institutions in exchange for freedom from cyberattacks and loss of credibility.

Publicity. The Internet has huge publicity potential, and it is often used for publicity. It can instantly address a worldwide audience or individuals. Osama bin Laden's use of television and the Internet to spread his message to kill all Americans after the start of the coalition bombing on Afghanistan is a good example. The United States immediately requested that bin Laden receive no further publicity. Terrorist groups place media access at the top of their strategic priority lists when addressing their causes.

Global freedom. Thanks to the Internet, no longer is terrorism contained to the state in which one hides. Electrons do not have to show passports.[6] Instead, the base for terrorist operations is usually not even located in the target country anymore.

Psychological effects. The Internet can be used to initiate psychological terrorism. The psychological aspect of the Internet is often overlooked. Not only can it cause panic due to its seeming credibility, but it also can be used for deception or disruption.

Deception. The Internet has changed the terrorist communications network from one with strong central control to one with no clear center of control because of its networked nature. Unwitting accomplices, such as hackers, can be used as surrogates without ever understanding the end result of their actions.

Covert operations. The Internet can be used to send messages surreptitiously, much like the invisible inks that al-Qaeda promotes as a low-tech alternative to communications in cyberspace. For example, reports indicate that Egyptian computer experts working in Afghanistan devised a

communications network to enable extremists to exchange information via the World Wide Web without fear of being caught posting messages on e-mail and electronic bulletin boards.[7] It is to this latter category that attention is now focused in light of the purported use of steganography and encryption on the Internet by bin Laden's al-Qaeda terrorist group.

Short message service (SMS) text is a cryptic text. An example would be STR AT 8 . . . TD, which could mean "strike at 8 today." The message in cryptic form can be sent from one cellphone to another via an SMS center. India's *Hindustan Times* reported in November on credible reports linking the use of SMS techniques to al-Qaeda and other terrorists groups.[8] SMS works by transmitting signals from a cellphone to the cellular operator's automatic SMS center. The center dials the SMS's destination number and puts the message in the queue. This technique may force governments to monitor SMS centers.

One author notes that, "if there is one thing the FBI hates more than Osama bin Laden, it is when bin Laden starts using the Internet."[9] He accuses bin Laden of hiding maps and photos of targets and of posting instructions on sports chat rooms, pornographic bulletin boards, and other websites. This practice is known as steganography, embedding secret messages in other messages to prevent observers from suspecting anything unusual. Messages can be hidden in audio, video, or still image files, with information stored in the least significant bits of a digitized file.


تواترت عليها الشواهد واطبق عليها
المنصفون ونحن نذكرها ليتذكر من
يتذكر، وليهلك من هلك عن بينة، ويحيا
من حيا عن بينة وهي:
اولا: منذ ما يربو عن سبع سنين
وامريكا تحتل اراضي الاسلام في القدس
بقاعها، جزيرة العرب، وتنهب خيراتها،
وتملي على حكامها وتذل اهلها، وترعب
جيرانها، وتجعل من قواعدها في الجزيرة
رأس حربة تقاتل بها شعوب الاسلام
المجاورة.
واذا كان في الماضي من جادل في
حقيقة هذا الاحتلال فقد اطبق على
وذلك حتى يتحرر المسجد الأقصى
والمسجد الحرام من قبضتهم، وحتى
تخرج جيوشهم عن كل ارض الاسلام
مثقولة الحد كسيرة الجناح عاجزة عن
تهديد اي مسلم، امتثالا لقوله تعالى
«وقاتلوا المشركين كافة كما يقاتلونكم
كافة». وقوله تعالى «وقاتلوهم حتى لا
تكون فتنة ويكون الدين لله».
وقوله تعالى «وما لكم لا تقاتلون في
سبيل الله والمستضعفين من النساء
والولدان الذين يقولون ربنا اخرجنا من
هذه القرية الظالم اهلها واجعل لنا من
لدنك وليا واجعل لنا من لدنك نصيرا».

A notional example of steganography on a photo from the celebrations in Washington, DC, after the Gulf War. While this scenario is notional, the "hidden" message is an actual excerpt from Osama bin Laden's first fatwa, or religious edict, instructing Muslims to kill Americans - including civilians - anywhere in the world where they can be found.

The FBI and terrorism authorities in the United States believe that bin Laden's network has used steganography in the past. So far, authorities have not said whether the terrorists who planned and carried out the events of 11 September used the technique. A few days before the attack, a team at the University of Michigan used a series of computers to search for images that might contain terrorist plans but found none. Instead, some FBI inves-tigators have traced hundreds of e-mail communications associated with the World Trade Center bombers that were sent from libraries or personal computers. They were written in English or Arabic and did not use encryption; they could simply be read openly.[10] Perhaps bin Laden's group was onto the fact that the FBI was watching for such hidden messages, so they used open lines to send messages, hoping these lines would not be so closely examined.

Encryption, on the other hand, relies on ciphers and codes to scramble messages. In a recent *USA Today* article, the author cites an unnamed U.S. official's claim that encryption has become "the everyday tool of Muslim extremists in Afghanistan, Albania, Britain, Kashmir, Kosovo, and other places, and that bin Laden and other Muslim extremists are teaching it in their camps in Afghanistan and Sudan."[11] In his testimony before Congress, former FBI director William Freeh complained about encryption but not steganography. Former Attorney General Janet Reno reportedly told a presidential panel on terrorism in 2000 that extremist groups are encrypting both e-mail and voice messages. An Israeli, Reuven Paz of the Institute for Counter-Terrorism, believes all terrorist groups are using the Internet to spread their messages. Most problematic for law enforcement authorities is that the Internet has 28 billion images and 2 billion websites.

Networks in general have received as much attention as the Internet in the past few years. Authors David Ronfeldt and John Arquilla introduced the term "netwar" several years ago. It refers to "an emerging mode of conflict at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age."[12] Netwar, then, appears to be an updated version of the old communist cell organization, a complex network in and of itself, which used dead drops and cutouts to deliver messages and conduct operations. In general, it was the more centralized predecessor of the netwar that Ronfeldt and Arquilla described. These networks offer not only the benefits of integration but also several risks and dangers including threats to freedom and privacy, new methods of surveillance, and several vulnerabilities to our national security infrastructure. More important, netwar empowers nonstate actors to organize into multiorganizational networks, offering the have nots a chance to work on a similar plane with the haves.[13]

Another excellent point Ronfeldt and Arquilla make is that a network's strength depends on five levels of functioning: organizational (design), narrative (story telling), doctrinal (strategies and methods), technological (information systems), and social (personal ties).[14] It appears that the al-Qaeda network functioned on all of these levels while planning and executing the attacks on 11 September. The network also makes the group appear leaderless and thus makes it harder to find those responsible. This is why the FBI has had such a difficult time tracking the killers and affixing blame on those responsible.

Ronfeldt and Arquilla appear overly reliant, however, on their description of "swarming" to explain what must be done to counteract terrorist netwar activities. In fact, they ignore their own advice. The authors define swarming as a structured, coordinated, strategic way to strike from all directions at a particular point or points by means with sustainable pulsing of force or fire.[15] In reality, swarming is not much different from the old concept of massing. In fact, in one of their examples, the authors cite critical mass strategies employed by a group of protestors. Even more important, the authors' reliance on swarming ignores their doctrinal functional level that recommends strategies and methods. Swarming is the only one offered when a myriad of other options should be considered. Theories such as China's 36 stratagems of war, and U.S. and Russian principles of war are only a few of those available. The latter would offer much more food for thought, such as blockade, deception, and reconnaissance, than simple swarming. Networks are not defeated by "keeping them on the run," as the authors conclude, but by conducting precision strikes on functioning nodes. The Chinese, for example, would recommend

using acupuncture war, that is, strikes against selected nodes to paralyze an enemy. If effective enough, a massed blow may never be needed.

De-terror-ence Suggestions

What can be done to thwart terrorists' use of Internet and Netwar techniques? Dr. John Chipman notes that "let us hope it [referring to yesterday's sense of emotional solidarity and today's shared political burden in the fight against terrorism] is handled with economic finesse, political savvy, military firmness and moral resolve in careful balance."[16] Chipman makes several excellent points that offer an initial look at a de-terror-ence plan:

- A diplomatic effort is needed to convince states supporting terrorism to desist from such activities or face the consequences, such as the Taliban is experiencing now.
- Commercial sanctions could be imposed on such states that "sup with the devil."
- The fight against terrorism must be combined with non- and counter-proliferation strategic campaigns, to keep sensitive weapons out of the hands of such groups. This will immediately bring to the table the debate over the role of export controls and direct action instead of arms control instruments, as some prefer.
- Major terrorist groups must be targeted, not just local groups.
- Creative approaches to information sharing must be developed, paying particular attention to countries outside of the Group of Eight-the United States, the United Kingdom, France, Italy, Japan, Russia, Canada, and Germany-NATO, and the European Union. This includes sharing intelligence for the protection of critical infrastructure.
- Challenges to civil liberties should be expected since heretofore restricted investigative tools associated with the Internet are required.
- Homeland defense commands will assert new authority over the de-terror-ence quest.
- Regional groups, such as NATO, must consider eliminating out-of-area distinctions since cyberattacks can come from anywhere.
- The world's leading banks must maintain coordinated action to shore up confidence and stabilize nervous markets. One cannot fight terrorism if one's house is crumbling.
- Muslim elements must help organize the current coalition's political elements, while the United States and Europe must expect to provide unprecedented economic, physical, and technical assistance. More parts of the developing world must be brought into the modern and post modern world.[17]

All nations at the international level need to cooperate with mutual legal assistance treaties, extradition, intelligence sharing, and uniform computer crime laws so investigation and prosecution can cross international borders. The UN General Assembly adopted resolution 53/70 in December 1998, which invites members to exchange views on information security issues and ways to fight information terrorism and crime.[18] Such de-terror-ence steps must continue to be explored at a much greater pace. Terrorists exploit the civilized world's objectivity and openness to support their causes. In the past, terrorist actions were more difficult to organize and execute because of issues such as distance and coordination. Today, those issues and a host of others have been eased, if not eradicated by information-age tools such as the Internet. The result is the emergence of a new, networked terrorist who can coordinate doctrine, narrative, organization, and loyalty often in plain view through the benefit of technology in the form of steganography

and encryption. This has made terrorist attacks more efficient and timely, and more difficult for law enforcement officials to recognize and expose.

These issues have motivated governments in only a few months to redirect attention and money to counter terrorism. The recent creation of a homeland defense czar in the United States, and recent legislation to allow law enforcement officials to more quickly move against and seize suspected terrorists are but two of the most apparent manifestations of this process. On the international arena, partnerships formed very quickly to fight the new threat, with Russian-U.S. cooperation to resolve basing issues in Central Asia being the best example.

While terrorism in the information age is far from being resolved, it is encouraging to witness the rapid development of methods and procedures to counter it. This effort must be further developed and refined over the coming months as many de-terror-ence options need to be discussed. On the other hand, it is important to watch the pulse of public opinion in the coming months. Cooperation and compromise among all leaders may hold the key to whether the fight against terrorism is successful.
;

1.This is the author's term, used here only to highlight the need for a plan devoted to deter a terrorist act.

2.U.S. Department of Justice, *Terrorism in the United States* (Washington, DC: Federal Bureau of Investigation, 1998).

3.Matthew G. Devost, Brian K. Houghton, and Neal A. Pollard, "Information Terrorism: Can You Trust Your Toaster?" The Terrorism Research Center (April 1996), 10.

4.Mark Pollitt, "Cyberterrorism-Fact or Fancy?" Proceedings of the 20th National Information Systems Security Conference (October 1997), 285-89.

5.Michael R. Gordon, "Pentagon Corners Output of Special Afghan Images," *The New York Times* (19 October 2001), B2.

6.Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," The Terrorism Research Center, date unknown, 19, online at <www.terrorism.com/documents/denning-infoterrorism. html>.

7.John Arquilla, David Ronfeldt, and Michelle Zaninni, "Networks, Netwar, and Information Age Terrorism" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 65 and 66.

8.Saurabh Shukla, "Is Osama Using SMS to Brief his Sleeper Agents?" *Hindustan Times*, 11 November 2001, available online at <Hindustantimes.com>.

9.Declan McCullagh, "Bin Laden: Steganography Master?" online at <http://www.wired.com>.

10.Duncan Campbell, "How the Plotters Slipped U.S. Net: Spy Networks Failed to Detect E-Mail and Satellite Conversations Used to Plot the Attack on the U.S.," *The Guardian* (27 September 2001).

11.Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, 6 June 2001, online at <http://www.usatoday.com>.

12.David Ronfeldt and John Arquilla, "Networks, Netwars, and the Fight for the Future," *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, DC: RAND 2001, TBP), as downloaded from an e-mail file sent to the author.

13.Ibid.

14.Ibid.

15.Ibid.

16.John Chipman, "The Strategic Implications of Terror in the Information Age," International Institute for Strategic Studies Annual Conference Geneva, Switzerland, 12-15 September 2001, online at <http://www.iiss.org/pub/tx/tx01015.asp>.

17.UN Resolution 53/70, Development in the field of information and telecommunications in the context of international security (NY: UN Disarmament Resolutions, 53d General Assembly, United Nations, Department of the Economic and Social Affairs, December 1998).